# Telehealth Security Best Practices for CCHS Providers

**When speaking with patients and working on your own computer:**

- Work in a private area. If possible, lock your door to prevent walk-ins.
- Log off Epic when you leave your computer.
- Don't save data to your local computer or print anything with patient's information.
- Disable smart devices (Alexa, Nest) & digital assistants (Siri, Google) as they have been known to begin transcribing audio spontaneously.
- If you or the patient do not feel comfortable with doing any of the physical exam by video, bring the patient in for a face-to-face.
- We do not recommend performing breast or GU exams by video.
- One important issue is patient privacy in their own home. Ensure that the patient is in a private area. This is especially important when talking with a minor.
- If possible, ensure your home Wifi is secured with WPA2 or WPA3 encryption. Do not use WEP or WPA. In most cases, you'll need to log into your internet service provider's webpage if you need to change this (e.g. Xfinity, Comcast etc). Here's a link to a helpful article on this: https://www.cnet.com/how-to/5-settings-to-change-on-your-new-router/

References:
David Ginsberg
HIPAA Advisor to California Medical Association
dginsberg@privaplan.com

Compiled by B. Yoshi Laing, April 2020